RIPE NCC
RIPE NETWORK COORDINATION CENTRE

HTTPS in TAL URIs

Tim Bruijnzeels | 16 July 2017 | IETF 99

Trust Anchor Locator (RFC7730)

```
rsync://rpki.example.org/rpki/hedgehog/root.cer
rsync://rpki.example.org/rpki/warthog/root.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAovWQL2lh6knDx
GUG5hbtCXvvh4AOzjhDkSHlj22gn/1oiM9IeDATIwP44vhQ6L/xvuk7W6
Kfa5ygmqQ+xOZOwTWPcrUbqaQyPNxokuivzyvqVZVDecOEqs78q58mSp9
nbtxmLRW7B67SJCBSzfa5XpVyXYEgYAjkk3fpmefU+AcxtxvvHB5OVPIa
BfPcs80ICMgHQX+fphvute9XLxjfJKJWkhZqZ0v7pZm2uhkcPx1PMGcrG
ee0WSDC3fr3erLueagpiLsFjwwpX6F+Ms8vqz45H+DKmYKvPSstZjCCq9
aJ0qANT9OtnfSDOS+aLRPjZryCNyvvBHxZXqj5YCGKtwIDAQAB
```

Going Forward

```
https://rpki.example.org/rpki/hedgehog/root.cer
rsync://rpki.example.org/rpki/warthog/root.cer
```

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAovWQL2lh6knDx
GUG5hbtCXvvh4AOzjhDkSHlj22gn/1oiM9IeDATIwP44vhQ6L/xvuk7W6
Kfa5ygmqQ+xOZOwTWPcrUbqaQyPNxokuivzyvqVZVDecOEqs78q58mSp9
nbtxmLRW7B67SJCBSzfa5XpVyXYEgYAjkk3fpmefU+AcxtxvvHB5OVPIa
BfPcs80ICMgHQX+fphvute9XLxjfJKJWkhZqZ0v7pZm2uhkcPx1PMGcrG
ee0WSDC3fr3erLueagpiLsFjwwpX6F+Ms8vqz45H+DKmYKvPSstZjCCq9
aJ0qANT9OtnfSDOS+aLRPjZryCNyvvBHxZXqj5YCGKtwIDAQAB
```

Or even?

```
https://rpki.example.org/rpki/hedgehog/root.cer
https://rpki.example.org/rpki/warthog/root.cer
```

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAovWQL2lh6knDx
GUG5hbtCXvvh4AOzjhDkSHlj22gn/1oiM9IeDATIwP44vhQ6L/xvuk7W6
Kfa5ygmqQ+xOZOwTWPcrUbqaQyPNxokuivzyvqVZVDecOEqs78q58mSp9
nbtxmLRW7B67SJCBSzfa5XpVyXYEgYAjkk3fpmefU+AcxtxvvHB5OVPIa
BfPcs80ICMgHQX+fphvute9XLxjfJKJWkhZqZ0v7pZm2uhkcPx1PMGcrG
ee0WSDC3fr3erLueagpiLsFjwwpX6F+Ms8vqz45H+DKmYKvPSstZjCCq9
aJ0qANT9OtnfSDOS+aLRPjZryCNyvvBHxZXqj5YCGKtwIDAQAB

On TLS Certificate Validation

- Similar to the considerations in the RRDP document…

- Even if TLS Certificate Validation fails, the Relying Party can still verify that the retrieved certificate matches the **subjectPublicKeyInfo** on the TAL

My preference

- Move forward to https only
  - Trivial for CAs and easier to scale
  - One less place RPs need to call rsync (ever)

- Let RP use the first the https URI without any sort of validation issues if available

- If only sources with issues are available: retrieve, verify **subjectPublicKeyInfo** and use if the certificate is more recent than the one in cache

Practical Questions

- Adopt as WG item and discuss further?
- Probably substantive enough to warrant new RFC obsoleting 7730 (6 mentions of rsync, https validation considerations)
- Willing to author, but if current RFC7730 authors want to remain I am fine with that too

Questions